PRINCETON UNIVERSITY

Stephen Schultze
Associate Director, Center for Information Technology Policy
Princeton University

Sherrerd Hall, Room 304
Princeton, New Jersey 08544
609-258-2175
sjs@princeton.edu

Via Electronic Filing

July 12, 2012

Marlene H. Dortch
Secretary
Federal Communications Commission 445 Twelfth St., S.W.
Washington, DC 20554

Re:

Commercial Availability of Navigation Devices, CS Docket No. 97-80; Compatibility Between Cable Systems and Consumer Electronics Equipment, PP Docket No. 00-67; In the Matter of Basic Service Tier Encryption, Compatibility Between Cable Systems and Consumer Electronics Equipment, MB Docket 11-169, PP Docket 00-67.

Dear Ms. Dortch:

This letter is filed in response to the ex parte submission made on June 7 ("Comments") by Jonathan Friedman, Counsel for Comcast Corporation, regarding the results of a meeting between representatives from Comcast and Boxee.

In MB Docket 11-169, the Commission has asked whether to retain the basic service tier encryption prohibition first introduced in the *Compatibility Order* of 1994. Petitioners argue that the prohibition has been rendered unnecessary by subsequent changes to the MVPD device market, and Comcast recently filed Comments indicating that the company had devised a hypothetical solution for Boxee customers who would otherwise experience service loss.

The Commission should consider the basic service tier encryption prohibition in the context of its original adoption. The prohibition was indeed premised on eventual sunset, but only after specific subsequent developments in the market. Most notably, the *Compatibility Order* first contemplated "a digital cable standard […] that would allow for timely and efficient introduction of consumer products that could receive digital cable service."[1] The Commission nevertheless recently observed that:

> "Unfortunately, the Commission's efforts to date have not developed a vigorous competitive market for retail navigation devices that connect to subscription video services. Most cable subscribers continue to use the traditional set-top boxes leased from their cable operator; only 1 percent of the total navigation devices deployed are purchased at retail."[2]

---

[1] *See Implementation of Section 17 of the Cable Television Consumer Protection and Competition Act of 1992: Compatibility between Cable Systems and Consumer Electronics Equipment, 9 FCC Rcd 1981 (1994) ("Compatibility Order")*, ¶18.

[2] *See Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices, 25 FCC Rcd 14657 (2010) ("Third Report and Order and Order on Reconsideration")*, ¶4.

Even if CableCard eventually succeeds to some degree, it can provide only last-generation one-way technologies. Tru2way presents a regime of downloadable security content that allows for next-generation two way communications. Unfortunately, the regime places heavy restrictions on implementers, to the point that the effort appears to have failed.[3] Progress on AllVid has stalled. Even in the presence of provider-supplied set-top boxes, consumers often cannot connect the video output from these devices to third-party devices of their choosing, because such signals are encrypted when emitted by the set-top box. The necessary condition of a vigorous market for the consumer products envisioned in the *Compatibility Order* has not been realized.

Nevertheless, the Commission may wish to re-evaluate the encryption ban if there is a workable alternative that would clearly benefit consumers. The original *Compatibility Order* hints that, "the most desirable solution is for cable systems to use technologies that provide all authorized signals 'in the clear.'"[4] A proactive stance by the Commission on this issue could lead to a compromise that prohibits encryption-enforced non-interoperability *within the home*. The provider's set-top box (or CableCard) could still be responsible for decrypting signals in order to prevent service theft, but the video signal emitted from that device could be mandated to be "in the clear" to any device that wishes to interoperate.

This strategy appears to be consistent with the first stage of Comcast's proposal, in which an E-DTA would output (presumably unencrypted) basic tier content to a Boxee device. The second stage of the proposed solution, however, is inconsistent with this strategy in that it anticipates "the creation of a licensing path for integrating DTA technology into third-party devices." This licensing path seems reminiscent of DFAST, DTCP, HDCP, and other encryption schemes that are unrelated to "service theft" and instead impose certification regimes on third-party devices within the home (often limiting their compatibility, competitiveness, and freedom of their users).

Although most consumers may already receive basic tier channels via a set-top-box, the prohibition currently serves as a useful safety valve on faulty or over-aggressive content protection license regimes. For instance, CableCard certified third-party devices frequently cannot receive even the unencrypted channels that the consumer has purchased because of unpredictable copy protection flags, whereas Clear QAM tuners continue to receive these signals without issue.[5]

The Commission's decision in this matter should reflect consideration of not just the narrow question of whether specific companies could hypothetically create a work-around for some customers, but also the role of the encryption ban in the FCC's larger strategy for facilitating competitive video devices. If the Boxee device is able to receive an unencrypted video stream from an MVPD-provided device, why should this option not be available for all paid-for channels and to any other in-home devices? It is not a question of technical standards (HDMI is most ubiquitous, and protocols built on top of IP seem likely to grow in popularity), but rather a question of whether encryption and licensing schemes should be tolerated on these in-home streams.

---

[3] *See* Ben Drawbaugh, "Retail tru2way devices are officially DOA, even Panasonic stops trial." (July 29 2010): http://hd.engadget.com/2010/07/29/retail-tru2way-devies-are-officially-doa-even-panasonic-stops-t/

[4] *See Compatibility Order*, ¶19.

[5] These flags often take the form of CableCard Copy Control Information (CCI) bits, which are set inconsistently for the same channels across different MVPDs. *See, e.g.,* Dave Zatz, "The Best & Worst Cable Companies (For TiVo Owners)" (February 5, 2012): http://www.zatznotfunny.com/2012-02/the-best-worst-cable-companies-for-tivo-owners/

The compromise approach would allow MVPDs to encrypt all channels before they enter the home in order to prevent service theft, but would also require them to offer consumers true interoperability with third-party devices by leaving the set-top box outputs unencrypted. Such an approach is easily implementable compared to the endless technical proceedings and difficult waivers of the past 15 years. If set-top boxes must output content "in the clear" (or if third-party devices are legally permitted to decrypt it) the artificial non-interoperability of encryption within the home ends.

This proceeding provides a valuable leverage point for consumer choice in the third-party video device market, and the Commission should not too quickly concede to idealized industry agreements—particularly when those agreements are short on details and when they echo failed MOUs of the past.[6] The Commission's past concessions to in-the-home encryption schemes presumed that the complex resulting regimes would foster a vibrant market for third-party devices, and reserved the far simpler solution of mandating "in the clear" signals. The Commission should now consider applying this requirement to the output of set-top boxes, subject to its jurisdictional authority under Sections 624A and 629 of the Communications Act.

Sincerely,
/s/ Stephen Schultze
Stephen Schultze[7]

[6] Consider tru2way, and IEEE 1394 mandates.
[7] The preceding comments are entirely my own, prepared in my capacity as an independent academic, and do not necessarily represent the opinion of Princeton University or any other party.